UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of:

The premises known as the offices of Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 Account: jm970684@gmail.com	)	Case No. 5:20-mj-22

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota *(identify the person or describe the property to be searched and give its location)*:

See **ATTACHMENT A**, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Evidence of a crime in violation of 18 U.S.C. §§ 2251, 2252, 2252A, as described in **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before Feb. 12, 2020 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)*. ☐ until, the facts justifying, the later specific date of _____.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 1-29-2020 10:15am

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

cc: AUSA Sarah Collins
Kle

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
5:20-mj-22		

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date:

Executing officer's signature

Printed name and title

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of:

The premises known as the offices of Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043
Account: jm970684@gmail.com

Case No. 5:20-mj-22

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed *(identify the person or describe the property to be seized)*:

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2251, 2252, 2252A	Possession or receipt of Child Pornography

The application is based on these facts:

☒ Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.

☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

Applicant's signature

Michelle Pohlen, Special Agent Homeland Security Investigations
Printed name and title

Sworn to before me and:
☑ signed in my presence.
☐ submitted, attested to, and acknowledged by reliable electronic means.

Date: 1-29-2020

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DISTRICT

IN THE MATTER OF THE SEARCH OF: The premises known as the offices of Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 Account: jm970684@gmail.com	CR 5:20-mj-22 **REDACTED AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION**

State of South Dakota)
) ss
County of Pennington)

INTRODUCTION AND AGENT BACKGROUND

I, Michelle Pohlen, Special Agent with Homeland Security Investigations (HSI), and currently assigned to the Rapid City, South Dakota Resident Agent in Charge (RAC) Office, being duly sworn, states as follows:

1. I have been a Special Agent (SA) with HSI since March 2019. In September 2019, I completed the Homeland Security Investigations Special Agent Training (HSISAT) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. In June 2019, I completed the Criminal Investigator Training Program (CITP), also located at FLETC in Glynco, GA. Prior to becoming a Special Agent, I was employed as a Federal Air Marshal with the Federal Air Marshal Service (FAMS) for two and a half years. Prior to FAMS, I served as a Police Officer with the Savannah Chatham Metropolitan Police Department (SCMPD) in Savannah, Georgia for one and a half years. I received a Bachelor of Arts degree in Law Enforcement in 2014.

2. During my law enforcement career, I have been involved in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

3. I am aware that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the production, distribution, receipt and possession of visual depictions of a minor engaging in sexually explicit conduct, using any means or facility of interstate or foreign commerce, including by computer or utilizing the internet.

4. The facts set forth in this affidavit are based on my personal knowledge; knowledge obtained from other individuals, including other law enforcement officers; interviews of persons with knowledge; my review of documents, interview reports and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, no information known to me that would tend to negate probable cause has been withheld from this affidavit.

ITEMS TO BE SEARCHED FOR AND SEIZED:

5. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to a Google, Inc. account found during the investigation of an unknown subject utilizing the TARGET ACCOUNT, which is more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography), and which items are more specifically described in Attachment B. The specific Gmail account is: jm970684@gmail.com (also referred to in this affidavit as "Target Account").

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachments A and B:

a. "Chat," as used herein, refers to any kind of text communication transmitted over the Internet in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format, that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Cloud-based storage service," as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to access these files easily through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18

U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information, which a computer can interpret and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide

computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. "Electronic Storage Device" includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any "cloud" storage by any provider.

l. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and

uses separate control and data connections between the client and the server.

m. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

n. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows the user to send short text messages from one cell phone to another cell phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1),

means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

r. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON CHILD EXPLOITATION AND CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET, AND EMAIL

7. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers serve many functions for persons who exploit children online; they serve as a mechanism for meeting child-victims and communicate with them; they serve as a mechanism to get images of the

children and send images of themselves; computers serve as the manner in which persons who exploit children online can meet one another and compare notes.

b. Persons, who exploit children online, can now transfer printed photographs into a computer-readable format with a device known as a scanner and then distribute the images using email, like Gmail and Yahoo! Inc. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The user can easily transfer video files from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer with telephone, cable, or wireless connection. People can make electronic contact to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it

inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Persons can transfer child pornography via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The Internet affords individuals several different venues for meeting and exploiting children in a relatively secure and anonymous fashion.

e. Individuals also use online resources to exploit children, including services offered by Internet Portals such as Gmail and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where a user utilizes online storage is, evidence of child pornography can be found on the user's computer or external media in most cases.

8. Based on my training and experience and investigation in this case, I have learned the following about Google:

a. Google offers an e-mail service that is available free to Internet users called "Gmail." Stored electronic communications, including opened and unopened e-mail for Gmail subscribers may be located on Google's computers.

b. Google maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, e-mail transaction information, and account application information.

c. Subscribers can access their Gmail e-mail accounts by activating software on a device or computer, login in using unique usernames and passwords, and connecting to high-speed Internet computers called "servers" maintained and/or owned by Google. Subscribers also may be able to access their accounts from any other computer in the world through Google's web site on the Internet.

d. When a user sends any e-mail to a Gmail e-mail subscriber the email is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes it or until the stored e-mail exceeds the storage limit allowed by Google.

e. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination, usually through another subscriber's e-mail provider. Copies of sent e-mail are stored on Google's servers in the same manner as received e-mail, Google retains the email until the user

deletes it or exceeds the storage limit.

f. Even if the contents of the message no longer exist on the company's servers, Google may have records of when a subscriber logged into his or her account, when a message was sent or received, as well as technical routing information that law enforcement could use to determine who sent or received an e- mail.

9. From my training and experience, I am aware that Google's computers contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the computer accounts and/or files for information and the content of communications pertaining to the Target Account specified herein and in Attachment A, following the procedures described herein.

PROBABLE CAUSE

10. On January 2, 2020, Detective Elliott Harding received four cybertips from the National Center from Missing and Exploited Children (NCMEC): 59190015, 59738685, 59844348 and 60115237.

CYBERTIP 59190015:

11. The images in cybertip 59190015 were locked so Harding obtained a search warrant to unlock the files from the 7th Judicial Circuit, South Dakota. He learned the following:

Incident Information:
Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 11-12-2019 01:13:40 UTC.

Description of Incident Time: The incident date refers to the approximate date and time Google became aware of the reported material.
Suspect Name: Jay
Date of Birth: 08-27-2000

Email Address: dogeye17@gmail.com (Verified)
Email Address: jm970684@gmail.com

Additional Information Submitted by the Reporting ESP:
Google became aware of the reported content which was stored in Google Drive infrastructure
Uploaded File Information: Number of uploaded files: 72

12. Det. Harding investigated the IP addresses associated with cybertip 59190015 and learned the following: 209.159.232.149: Vast Broadband; 45.33.129.40: CloudMosa; 107.178.38.28: CloudMosa; 109.169.63.48: Iomart Hosting Limited.

13. Per Harding: Within this portion of the CyberTip, it provided many Login IP addresses from 2/10/19 and 11/4/19. Many of the IP addresses listed were 209.159.232.149. There were single instances of IP addresses 45.33.129.40, 104.244.78.233 and 107.178.38.28. There were two instances of 109.169.63.48.

14. Det. Harding observed the images associated with cybertip 59190015. He observed a total of 71 files constituting child pornography. The images included a video of a 7-10 year old girl being anally raped; a picture of a 4-6 year old girl inserting her finger into another girl, of similar age's vagina while a male ejaculated into one of the girl's mouth; a picture of a 4-5 year old girl with an unknown object inserted in her vagina and anus; a video of a 3-5 year old girl digitally manipulating an adult penis; a video of a 2-4 year old being manipulated so her finger went in and out of her vagina; a video of a man inserting an

unknown object into the vagina of a 6-8 year old; and a video of one 3-5 year old licking another like-aged female's anus and buttocks.

CYBERTIP 59738685:

15. NCMEC provided the following information regarding cybertip 59738685:

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)

Incident Time: 11-20-2019 08:00:59 UTC

Description of Incident Time: The incident date refers to the approximate date and time Google became aware of the reported material.

Suspect
The information under the Suspect heading was the same as CyberTip 59190015 mentioned above.

Additional Information Submitted by the Reporting ESP
Google became aware of the reported content which was stored in Google Drive infrastructure

Uploaded File Information
Number of uploaded files: 4

16. Det. Harding observed four images of child pornography related to this cybertip. The images included a picture of a 6-9 year old with her genitals partially exposed; a video of a 6-9 year old girl exposing her vagina; a picture of a 2-4 year old girl squatting and exposing her vagina with a sucker in her mouth; and a picture of a 6-8 year old girl exposing her vagina and breasts.

CYBERTIP 60115237:

17. Det. Harding learned that in cybertip 60115237, Google reported

Anime/Drawing/Virtual Child Pornography to NCMEC: **Incident Information**

Incident Type: Child Pornography (possession, manufacture, and distribution)

Incident Time: 11-26-2019 03:41:35 UTC
Description of Incident Time: The incident date refers to the approximate date and time Google became aware of the reported material.

Suspect: The information under the Suspect heading was the same as CyberTip 59190015 and 59738685 mentioned above.

Additional Information Submitted by the Reporting ESP: Google became aware of the reported content which was stored in Google Drive infrastructure
Uploaded File Information: Number of uploaded files: 1.

18. There was one file contained in this cybertip and it was a video of animated child pornography of a 5-7 year old girl in various states of nudity and engaging in masturbation with playground equipment and also engaging in sexual intercourse with a like-age male.

CYBERTIP 59844348

19. Detective Harding received a fourth cybertip related to the same user as the three described above. The following is the information he received from NCMEC:

Incident Information
Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 11-22-2019 03:11:39 UTC
Description of Incident Time: The incident date refers to the approximate date and time Google became aware of the reported material.

Suspect: The information under the Suspect heading was the same as CyberTips 59190015, 59738685 and 60115237 mentioned above.

Additional Information Submitted by the Reporting ESP: Google became aware of the reported content which was stored in Google Drive infrastructure

Uploaded File Information: Number of uploaded files: 1

20. Det. Harding reviewed the image associated with this cybertip. He described it as a photo of an 8-11 year old girl, standing on a couch with her genitals and breasts exposed.

21. On January 9, 2020, Det. Harding sent a request to HSI Analyst Amber Cooper asking her to identify the suspect based on the information provided in the four cybertips mentioned above. Analyst Cooper subpoenaed Vast Broadband regarding the IP address 209.159.232.149 which made up the majority of the suspect login IP addresses. Vast returned the following information:

[redacted]

22. Analyst Cooper reviewed obituary information published online provided the following associated family member names:

[redacted]
James Miller (the suspect)

23. Analyst Cooper conducted a driver's license inquiry which showed James Miller ([redacted]) lived at [redacted].

24. She also ran a criminal history inquiry, which provided that James Miller had been arrested for solicitation of a minor and the case is currently pending. Det. Harding reviewed the police reports related to that offense which confirmed that Miller lives at the above address. The allegations were that in the

summer of 2018, Miller separately approached three girls, one 11 years old and two 12 years old, playing around his apartment complex and asked to take pictures of them. One of the girls indicated that Miller asked to take pictures of her breasts and vagina.

25. Officers investigating the solicitation matter interviewed Rebecca Miller and James Miller at their home. Rebecca invited the officers into the apartment and retrieved James from a bedroom. Upon being asked if he was willing to participate in an interview, James indicated that he would first have to pause his computer game and returned to the room. James denied asking the girls for pictures. Rebecca indicated that despite James being an adult, she had guardianship of James because he is autistic and cannot make decisions for himself.

26. All four of the cybertips were associated with the same email accounts, which were dogeye17@gmail.com and jm970684@gmail.com (SUBJECT ACCOUNT). Analyst Cooper issued subpoenas to Google to get user information regarding dogeye17@gmail.com. Google responded that email's recovery email was the jm970684@gmail.com account and the user's name for that account was "James Miller".

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

27. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information (including the content

of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

JURISDICTION

28. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a "district court of the United States (including a magistrate judge of such court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

REQUEST/JUSTIFICATION FOR ORDER OF NONDISCLOSURE

29. The United States respectfully applies for an order of nondisclosure to Google, Inc. under 18 U.S.C. § 2705(b) regarding the following account: jm970684@gmail.com. The United States is seeking this search warrant for subscriber information, including all names, addresses, IP addresses, including historical, telephone numbers, other email addresses, information on length and types of services and any means of payment related to these accounts under the authority given by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Based on § 2703(c)(3), the United States is not required to provide notice to the subscriber. Under § 2705(b), the United States may apply to the court for an order commanding Google, Inc. not to notify the subscriber of the existence of the search warrant. The court may decide what length of time shall apply to the order of nondisclosure if the court determines the notification to the subscriber

could result in one of the five factors listed in the statute, which includes destruction of or tampering with evidence. 18 U.S.C. § 2705(b)(3). The basis for the request is that such disclosure could cause any person with access to the accounts, or any related account or account information, to tamper with or modify the content or account information and thereby destroy or tamper with evidence and otherwise seriously jeopardize the investigation. Especially due to the ease of access to Google, Inc., persons can modify its content with internet access and sufficient account information. As such, the United States respectfully requests this Court enter an order commanding Google, Inc. not to notify the user of the existence of this warrant.

REQUEST FOR SEALING OF MATTER

30. I request that the Court order sealing this case until further order of the Court. The documents filed in the case discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

LIMIT ON SCOPE OF SEARCH

31. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION

32. Based on my training and experience, and the facts as set forth in

this affidavit, there is probable cause to believe that on computer systems owned, maintained, controlled and/or operated by Google, Inc., there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic accounts described in Attachment A. The facts outlined above show that the Google, Inc. account, listed in Attachment A has been used for the exploitation of children using the internet including violations of 18 U.S.C. § 2422(b) (enticement of a minor using the internet), which items are more specifically described in Attachment B. There is probable cause to believe that the unidentified user of the Gmail account, exploited minors using the internet and thereby violated the aforementioned statutes in the District of South Dakota and elsewhere. The account is the subject of this warrant affidavit. The account is jm970684@gmail.com.

40. Law enforcement agents will serve the warrant on Google, Inc., who will then compile the requested records at a time convenient to it, so there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

41. For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of

federal criminal law. Additionally, I request authority to serve the warrant on Google, Inc. via the internet and to allow Google, Inc. to copy the data outside of this agent's presence.

RETURN COMPLIANCE BY GOOGLE, INC.

42. Google's policies prohibit mailing or emailing child pornography to law enforcement in response to a search warrant, instead requiring a law enforcement officer to personally appear and collect contraband materials, unless the means of production is explicitly described in that search warrant. Specifically, Google requires the Court order the disclosure, notwithstanding 18 U.S.C. § 2252A or similar statute or code.

Dated: 1/29/2020

Special Agent Michelle Pohlen
Department of Homeland Security
Investigations

Sworn to before me and:
☒ signed in my presence.
☐ submitted, attested to, and acknowledged by reliable electronic means.

this 29th day of January, 2020

Daneta Wollmann
United States Magistrate Judge

ATTACHMENT A
Property to Be Searched

This warrant applies to the contents of and information associated with the following Gmail email account, under an account known to be stored at the premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043: jm970684@gmail.com.

ATTACHMENT B
Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Google, Inc. (the "Provider") to facilitate execution of the warrant:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google Inc., including any emails, records, files, logs, or information that have been deleted but are still available to Google Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 14, 2020. Google Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A, including any information contained in the email account which is helpful to determine the accounts' user's or owner's true identity:

a. The contents of all e-mails associated with the account, from the time of the account's creation to the present, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each e-mail;

b. The contents of all Instant Messages (IM) associated with the account, from the time of account's creation to the present, including stored or preserved copies of IMs sent to and from the account, IM attachments, draft IMs, the source and destination addresses associated with each IM, the date and time at which each IM was sent, and the size and length of each IM;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP addresses used to register the account, all log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of services utilized;

e. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between Google Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I that was created or saved after the creation of the account that is the subject of this warrant and that constitutes contraband or fruits, evidence or instrumentalities of violations of 18 U.S.C. § 2422(b), enticement of a minor using the internet, including, for the account or identifiers listed on Attachment A, information pertaining to the following matters:

a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, or attempting or conspiring to do so;

b. Any person knowingly distributing, receiving, or possessing child pornography as defined at 18 U.S.C. § 2256(8), or attempting or conspiring to do so;

c. Any person knowingly persuading, inducing, enticing, or coercing any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged, or attempting to do so;

d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, or events relating to the crime under investigation and to the email account owner or user;

e. Evidence indicating the email account users or owner's state of mind as it relates to the crime under investigation;

f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

g. Records relating to who created, used, or communicated with the electronic account or identifier listed in Attachment A about matters relating to the criminal activity listed above, including identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses, including records that help reveal their whereabouts.

2. Credit card information and money wire transmittal information, including bills, payment records, and any receipts, for payments to third party money remitters, including Xoom.com, Western Union, PayPal, and MoneyGram.

3. Evidence of who used, owned, or controlled the account or identifier listed on Attachment A, including evidence of their whereabouts;

4. Evidence of the times the user utilized the account or identifiers listed on Attachment A;

5. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifier listed on Attachment A and other associated accounts.

III. Information Regarding Search Warrant Compliance by Google:

Google shall disclose responsive data, if any, by sending to:

Special Agent Michelle Pohlen
Department of Homeland Security Investigations
1516 Fountain Plaza Drive
Rapid City, SD 57702
Michelle.A.Pohlen@ice.dhs.gov

Google shall use the United States Postal Service or another courier service to disclose the responsive data, notwithstanding 18 U.S.C. § 2252A or similar statute or code. In the alternative, Google may make the responsive data available to Special Agent Pohlen by use of its law enforcement website.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google Inc., and my official title is _____. I am a custodian of records for Google Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google Inc.; and

c. such records were made by Google Inc. as a regular practice.

I further state that this certification is intended to satisfy Rules 902(11) and (13) of the Federal Rules of Evidence.

_____ _____

Date Signature